BBRI Digital Literacy Program

An initiative of Broadband Rhode Island

# Internet Safety & Privacy Basics

*Estimated Classroom Time: 2 hours*

## Overview

The Internet's immense influence and ever evolving technologies, coupled with the explosion of social media, have made users far more exposed to security threats and privacy intrusions.

This module will introduce you to some of the common types of threats you may encounter while online and while using email. Internet safety and online privacy is of major concern for all Internet users, but can be particularly troublesome to new users.

This module requires a delicate balance by the instructor to deliver a class that is cautionary, but not excessively alarming. It is important that by the completion of this module, the student comprehends the public nature of the Internet, primary cautions about being online, and some practices that can reduce some of the threats they will face.

## Module Outline

| Module Section | Lesson Title | Suggested Classroom Length |
|---|---|---|
| **A** | Internet Safety & Privacy – Part A | 60 minutes |
| | ***Class Break*** | 10 minutes |
| **B** | Internet Safety & Privacy – Part B | 50 minutes |

## Key Objectives

- NAVIGATION SKILLS: Students will build on the navigation skills they learned in Modules 1 and 2 by learning how to navigate dynamic websites, while applying safety and privacy practices.

- SEARCH SKILLS: Students will build on their search skills by practicing searching and browsing using safety and privacy practices, thus developing an Internet safety mindset.

- COMMUNICATION SKILLS: Students will build on the email communication skills learned in module 3 by recognizing basic common threats, and ways to reduce risk when communicating via email.

## Key Concepts and Vocabulary Terms

- Username
- Password
- Challenge Security Questions
- Public Data vs. Private Data
- https: vs. http:
- Logoff
- Phishing (Scamming)
- Viruses
- Worms
- Trojans
- Anti-Virus Software
- Parental Controls

# Internet Safety & Privacy – Part A

## PRE-CLASS PREPRATION TIPS

- Print out any handouts or visual aids you plan to use.
- Set the classroom browsers to the same homepage, preferably Google or another search engine.
- Review Internet examples that you plan to use before class to make sure the information you are presenting is current.
- Do a "tech check" of all equipment to be used during class to make sure all devices are working properly. A full Pre-Class Preparedness Checklist is available on the Digital Literacy Portal website.

Identify key concepts and examples from modules 1 & 2 (navigation & searching) to use as a quick review prior to introducing new material. Review navigation and searching briefly with students prior to beginning Step 1.

## STEP 1: INTRODUCE AND ASK

Begin the class by **INTRODUCING** students to the public nature of the Internet and typical online safety and privacy threats (simple passwords, email phishing scams, etc.) they may encounter while online.

**ASK** students for a few examples from their own experiences re: Internet security concerns. React to and discuss these examples briefly.

Then, **ASK** students to react to examples that you provide.

- **INTRODUCE** the concept of passwords and how to determine their relative "strength"
- **INTRODUCE** the concept of using challenging security questions.
- **INTRODUCE** the concept of phishing scams, and explain the sophisticated and deceiving nature of these criminal acts.

## STEP 2: DEMONSTRATE THREE TYPES OF PRACTICES TO MINIMIZE THREATS

The in-class exercise for this module focuses on developing students' awareness and ability to identify potential safety threats, and some standard countermeasures to reduce them. Using examples that are interesting to the class (possibly related to some of their own stated concerns), **DEMONSTRATE** the following:

1. **DEMONSTRATE** how to create a secure password. Play a pre-selected video on password security. Some suggestions:
   - http://www.youtube.com/watch?v=oOZIWxKnyVU (Common Craft)
   - http://www.youtube.com/watch?v=nyP2BcP4uoo (Googolplex)

   **Discuss** students' reactions or questions from the video.

   Next, **DEMONSTRATE** how to check for a password's level of "strength". Suggested format: Ask the students to list some possibly weak passwords and then compare to the list of 25 worst (most common) passwords of 2012, provided below.

### 25 Most Common (**Worst**) Passwords of 2012

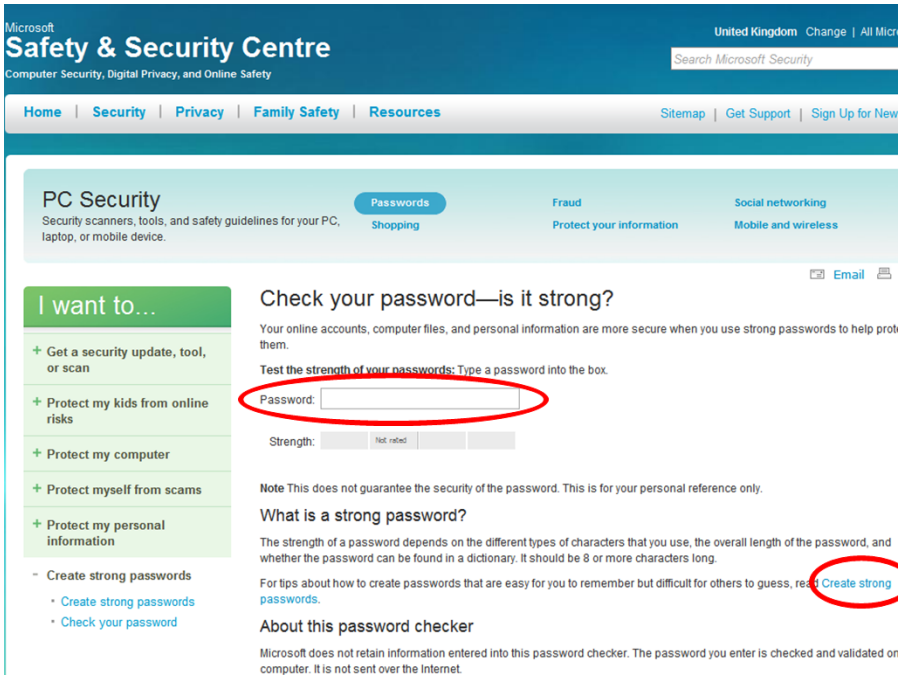
Source: SplashData, Inc.

| | | |
|---|---|---|
| 1…password | 10…baseball | 18…shadow |
| 2…123456 | 11…iloveyou | 19…Ashley |
| 3…12345678 | 12…trustno1 | 20…football |
| 4…abc123 | 13…1234567 | 21…jesus |
| 5…qwerty | 14…sunshine | 22…Michael |
| 6…monkey | 15…master | 23…ninja |
| 7…Letmein | 16…123123 | 24…mustang |
| 8…dragon | 17…welcome | 25…password1 |
| 9…11111 | | |

**Discuss** results and students' ideas about weak & strong passwords.
Topics to fuel discussion could include: 1) Minimum and maximum lengths of passwords 2) Can two people have the same password 3) The terms "user name" and "user id" and how they are associated with passwords.

Now, login to Microsoft's "Password Checker" program:
https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx
And as you enter some sample passwords, tell the students the combinations that you are trying as the strength meter moves from "weak" to "strong" to "best" (Think out loud).

Then, have the students follow along and try their own ideas for passwords.
**Discuss** results and review key ideas about passwords.




2. **DEMONSTRATE** the use of Security Challenge Questions and the reasons for their use.
   - http://en.wikipedia.org/wiki/Security_question
   - http://www.goodsecurityquestions.com/
   - http://www.youtube.com/watch?v=jTBL1kOzs2s (video)

**Discuss** students' reactions and questions.

Provide some examples of good and poor security questions, and then ask the class to add to each list.

**Good** – Answers that will not change over time and are not easily researched

In what city did you meet your spouse/significant other?
What is the name of your favorite childhood friend?
In what city or town did your mother and father meet?
Where were you when you had your first kiss?

**Poor** – Answers that are fairly easy for others to know or research

What is the name of the High School you graduated from?
What is your pet's name?
In what year was your father born?
What is your mother's maiden name?

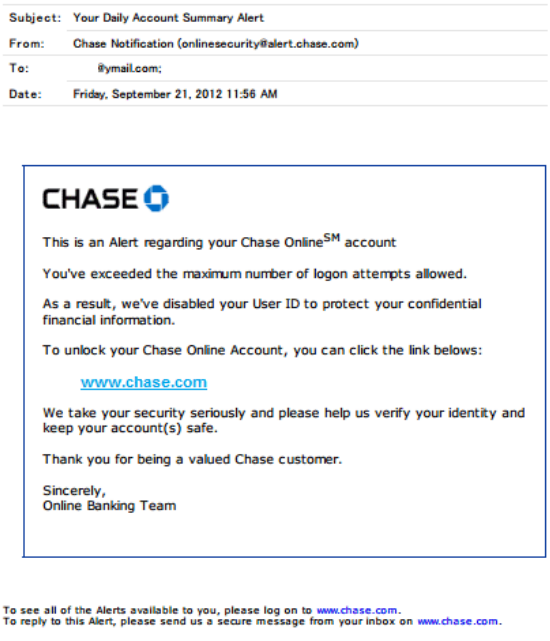
Have students write down a few good security questions they might want to remember.

3. **DEMONSTRATE** how to identify a Phishing Scam and some best practices to prevent or neutralize this type of threat. Discuss what "Phishing" means. You can play this great 3 minute video on Phishing: http://www.youtube.com/watch?v=3DN17ANbGdU

   **Discuss** with the class some of the basic ground rules for avoiding phishing scams:

   - **Don't email personal or financial information.** Email is not a secure method of transmitting personal information.
   - **Do not click on links in emails or reply to suspicious emails … independently open a browser and type in the website address**. This way, you control what sites you visit. Do not let a phisher direct you to a false site.
   - Only provide personal or financial information through an organization's website if you typed in the web address yourself and you see signals that the site is secure, like a URL that begins with **https** (the "**s**" stands for **secure**). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
   - **Be very cautious about opening attachments and downloading files from emails**, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security.
   - **Be cautious** about email messages that come from people or places you do not know. They could be "Phishing" for you. Scammers sometimes use mail or contact lists that are not protected – be sure that you know who you are getting email from.
   - **Be cautious** of messages with no subject, or messages that are too general – they could be phishing for you. If you suspect that a friend did not send a message, email them in a separate message and ask. Sometimes other's email addresses can be "pirated" by scammers.

Provide a few examples of phishing emails that you can show on screen or provide handouts, here are three examples:



Subject: Your Daily Account Summary Alert
From: Chase Notification (onlinesecurity@alert.chase.com)
To: @ymail.com;
Date: Friday, September 21, 2012 11:56 AM

CHASE

This is an Alert regarding your Chase Online[SM] account

You've exceeded the maximum number of logon attempts allowed.

As a result, we've disabled your User ID to protect your confidential financial information.

To unlock your Chase Online Account, you can click the link belows:

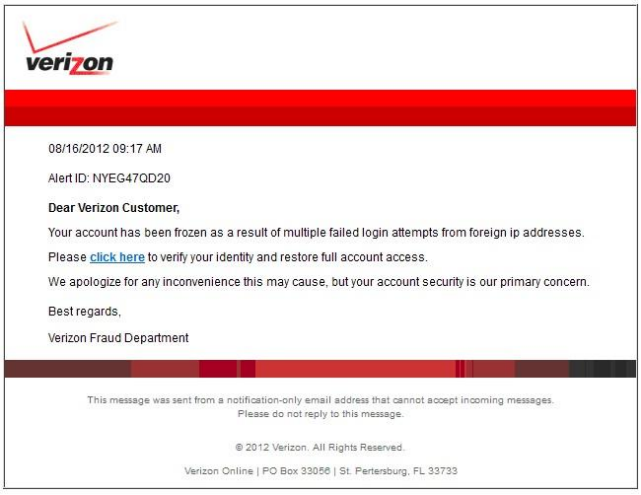
www.chase.com

We take your security seriously and please help us verify your identity and keep your account(s) safe.

Thank you for being a valued Chase customer.

Sincerely,
Online Banking Team

To see all of the Alerts available to you, please log on to www.chase.com.
To reply to this Alert, please send us a secure message from your inbox on www.chase.com.



verizon

08/16/2012 09:17 AM

Alert ID: NYEG47QD20

Dear Verizon Customer,

Your account has been frozen as a result of multiple failed login attempts from foreign ip addresses.

Please click here to verify your identity and restore full account access.

We apologize for any inconvenience this may cause, but your account security is our primary concern.

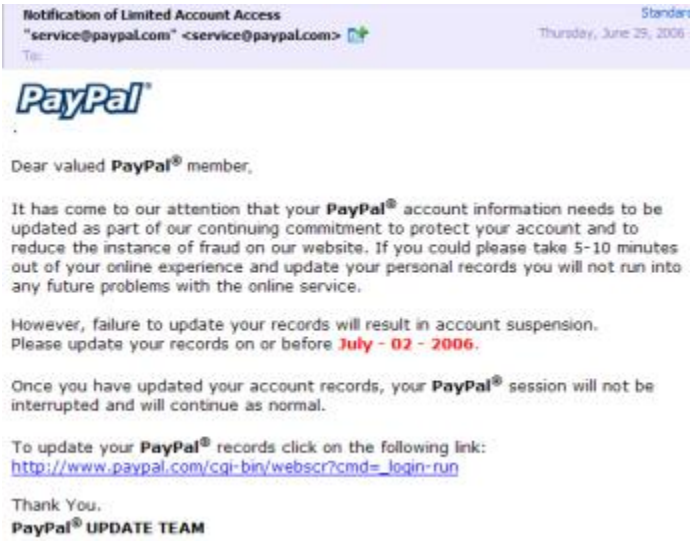
Best regards,

Verizon Fraud Department

This message was sent from a notification-only email address that cannot accept incoming messages. Please do not reply to this message.

© 2012 Verizon. All Rights Reserved.

Verizon Online | PO Box 33056 | St. Petersburg, FL 33733



Notification of Limited Account Access
"service@paypal.com" <service@paypal.com>
Thursday, June 29, 2006

PayPal

Dear valued **PayPal®** member,

It has come to our attention that your **PayPal®** account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before **July - 02 - 2006**.

Once you have updated your account records, your **PayPal®** session will not be interrupted and will continue as normal.

To update your **PayPal®** records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Thank You.
**PayPal® UPDATE TEAM**

## STEP 3: CLASS DISCUSSION OF SAFETY & PRIVACY PRACTICES

Ask students to **DISCUSS** the examples provided above or that you have prepared before class. Ensure the discussion includes suggested best practices to guard against the demonstrated threats.

# Internet Safety & Privacy – Part B

## STEP 1: INTRODUCE AND ASK

Begin Part 2 by **INTRODUCING** students to some additional realities of Internet safety and privacy; specifically what the differences are between publically available and private information.

- **INTRODUCE** the concept of public websites and private/secure websites.
- **INTRODUCE** the concept of http: vs. https.
- **INTRODUCE** the concept of logging OFF public/shared computers and Wi-Fi networks
- **INTRODUCE** the concept of Parental Controls
- **INTRODUCE** the concept of malware (viruses, worms, & Trojans)

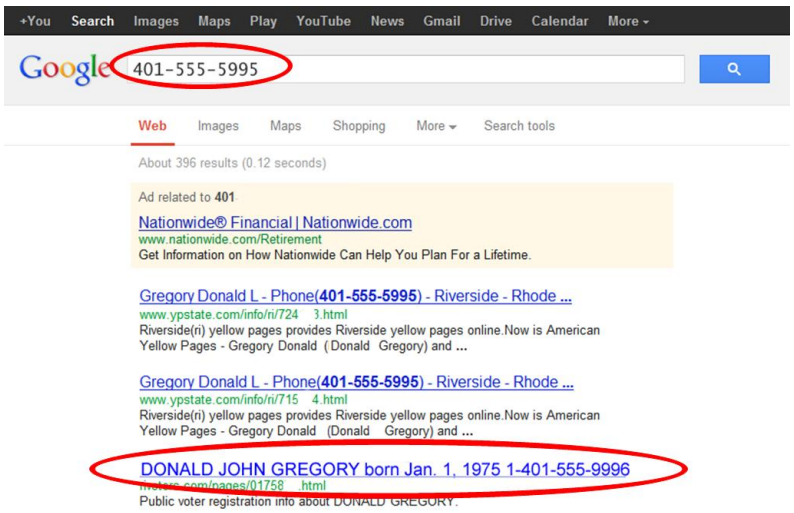
Then, **ASK** students to react to examples that you provide. **Discuss** their ideas.

## STEP 2: DEMONSTRATE THE THREE TYPES OF PRACTICES SHOWN BELOW TO HELP KEEP PRIVATE INFORMATION SECURE

The in-class exercise for this module should focus on developing students' awareness and ability to identify public vs. private information, and how each affects user privacy.

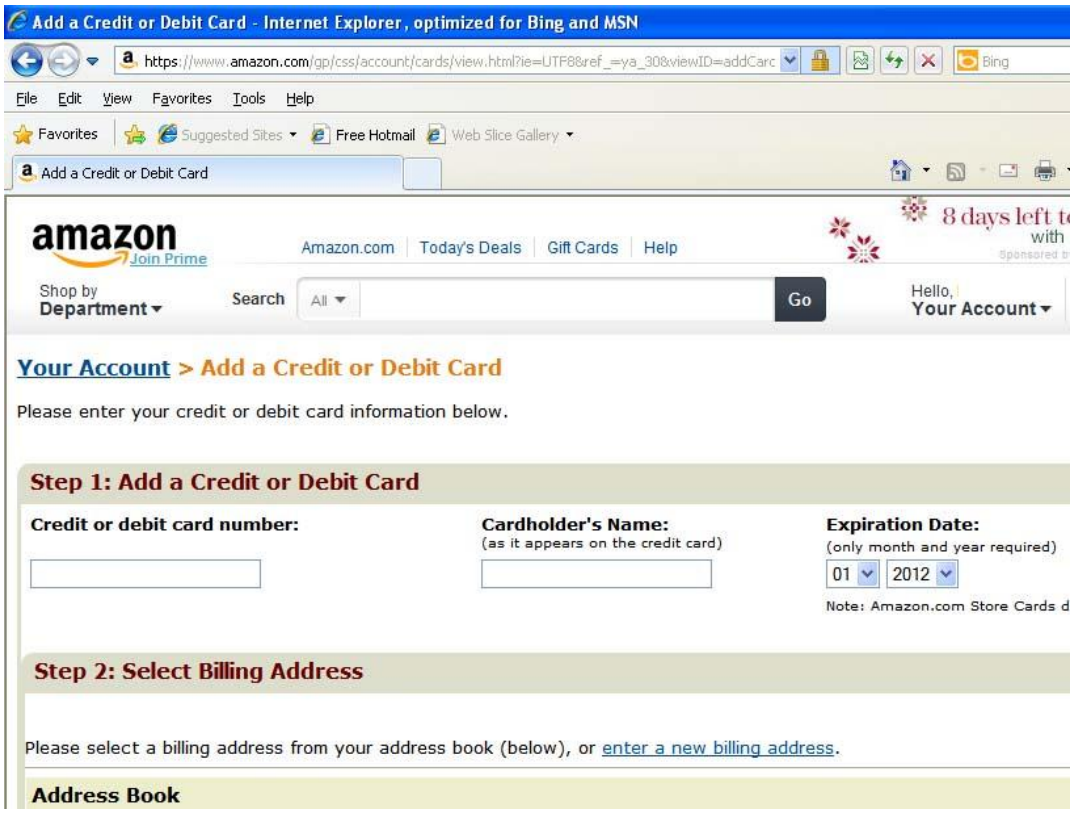
A suggested analogy to share with the class would be how **public** information online is like reviewing personal information in a bank lobby, compared with using a safe deposit box and secure vault room to view financial or important **private** information. Using examples that are interesting to the class, **DEMONSTRATE** the following:

1. **DEMONSTRATE** how to check to see what public information is available on the Internet. Using a search engine like Google, enter terms such as your name, email address, home and work address, and phone number in a variety of ways.



Explain how there are two types of information that exist online.

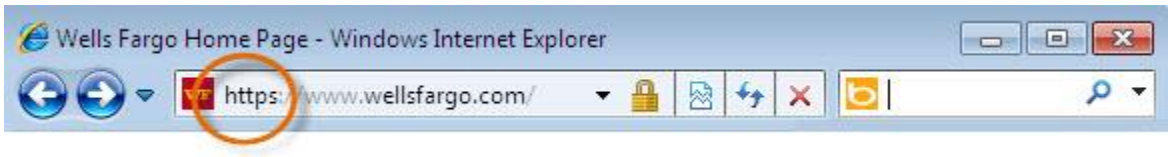
- **Public data** is collected from sources such as the US Census, voter registration, Division of Motor Vehicles, organizational memberships, tax assessor, telephone directories, etc. (The graphic above shows Public data for Donald John Gregory that is available because of voter registration records.)
- **Private data**, when entered into a computer, becomes **volunteered data**. This personal information is anything that you, as an online user, provide via email, website sign-up forms, Facebook posts, etc. (The graphic below shows an eCommerce sign-up page that is requesting private financial information.)




2. **DEMONSTRATE** how to identify whether a site is secure for input of financial transactions or important personal information.

Before sending any sensitive or financial information online, you want to know that you are communicating with a secure site. Secure sites make sure that all information you send is protected as it travels across the Internet.

Web addresses either begin with **http** or **https**. If the address is **https (the "s" stands for secure),** then the information you are sending is **encrypted** (secretly coded) and will look like gibberish if intercepted by cybercriminals.



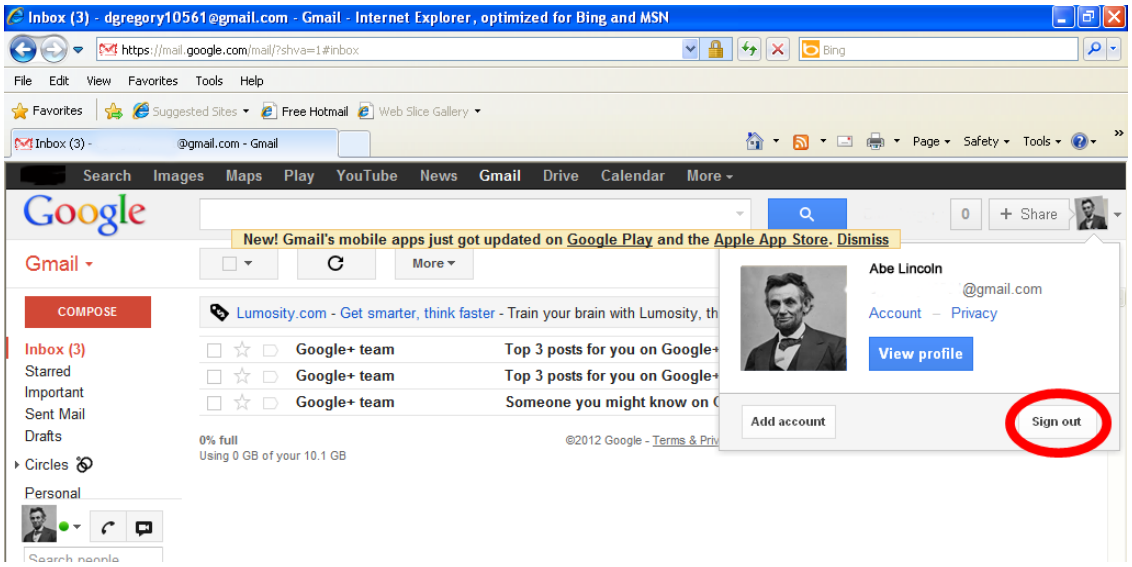

You can also point out that in the Amazon.com address used earlier in this lesson, the URL was a secure **https:** site.

3. **DEMONSTRATE** how to log off publicly used computers and Wi-Fi networks and explain the importance of this practice.

Show how if you fail to sign out of your email account or website that you were logged into, the next person has full access to all your secure information.

Log onto your Google email account and then minimize your screen. You can then demonstrate by walking away from the computer and then come back to it pretending to be another person and provide some examples of what could happen now that a stranger has access to your Google account: 1) Read your personal/financial information 2) Sending email etc…

Below is an example of how to log off from a public website.




4. **DEMONSTRATE** and provide a brief overview of "Parental Controls" and how they are best used to help keep children safe while being online.

Parental Controls allow parents to monitor and implement learning time into the computing time of children.

For a Windows 7 overview of Parental Controls you can show this video: http://www.youtube.com/watch?v=NQvusEhpHcY

**Discuss** students' questions about parental controls.

5. **DISCUSS** the three major types of computer malware (malicious software) and what resources are available to learn more about how to safeguard against such threats.

A good video to play for the class is: http://www.youtube.com/watch?v=t0M55k8Trq4

**Discuss** each (similarities and differences)

***Virus:*** malicious software code attaching itself to a host (existing) program
***Worm:*** stand-alone software code or program that does not need a host file
***Trojan:*** a program that is downloaded and opened that seems safe, but has malicious software hidden inside the code.

**Discuss** prevention measures for each. Three suggested topics are: 1) Update operating system software patches frequently 2) Use anti-malware software 3) Ensure a firewall is installed on your computer.

This topic will usually generate a lot of questions from students relating to their own situations. Consider managing shared experiences with guiding questions like: "*Is there one instance when you experienced malware? What was the result?"* This should help keep the direction of the discussion on track.

## STEP 3: REVIEW AND APPLY

Towards the end of class, recap the 8 practices covered in this module and remind students to keep security and privacy primary in their mind whenever going online. You may also encourage them to review and practice the exercises, at the following links, at home or wherever they have access to a computer.

**8 Practices covered in this module:**

- Creating strong passwords
- Choosing better challenging security questions.
- Rules to guard against phishing scams
- Check for your publicly available information
- Awareness of http vs. https, and what a secure site provides
- Logging off public computers and Wi-Fi networks
- How to use Parental Controls
- Basic prevention measures for Viruses, Worms, & Trojans

Additional helpful videos and resources on Internet security

- GCF Learnfree.org, Internet Safety
- GCF Learnfree.org, Beyond Email, All About Communicating Online
- Microsoft's, How to create strong Passwords
- Onguardonline.gov, Online Security and Privacy Site

# Disclaimer

Internet Safety and Privacy is a serious and extensive subject. By accessing, viewing, or otherwise using any of the information created, collected, compiled and provided here, you agree to be bound by these terms and conditions. The information provided here is intended to be an overview and introductory guide for instructors on how to address the topic with your students. In providing this information, we have attempted to be as accurate as possible. However, we make no claims, guarantees or promises about the accuracy, currency, or completeness of the information provided and we make no express or implied warranties of any kind or nature regarding the information. You understand and agree that we shall not be liable for any type of damages whatsoever whether or not we have been advised of or should have been aware of the possibility of such damages.